MBX DRIVER SUITE 5.00 SP2

Windows® XP SP2 Compatibility Issues

Technical Support Document

Document last revision date August 2, 2004

TABLE OF CONTENTS

INTRODUCTION

Recently, Microsoft made *Windows XP SP2 (RC2)* available for download at the Windows XP SP2 (RC2) Technical Preview Program (http://www.microsoft.com/technet/prodtechnol/winxppro/sp2preview.mspx). The goal of Windows XP SP2 – as described by the Microsoft website – is to introduce "a set of security technologies to help improve the ability of Windows XP-based computers to withstand malicious attacks from viruses and worms." Microsoft provides a very detailed description of Windows XP changes in its Changes to Functionality in Windows XP SP2 (http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx) document.

Cyberlogic has recently discovered minor compatibility issues between the *MBX Driver Suite 5.00 SP2* and *Windows XP SP2 (RC2)*. These issues arose because Microsoft improved Windows XP's default network security configurations. Fortunately, these compatibility issues are limited to the *Ethernet MBX Driver* and *Remote MBX Driver.* Furthermore, users may easily correct these issues without overly exposing their systems to malicious network attacks.

This document provides simple methods to correct the compatibility issues that have arisen between the *MBX Driver Suite* and *Windows XP SP2 (RC2)*. It is divided into the following sections:

Note: This procedure is tested only with Windows XP SP2 (RC2). Although Cyberlogic does not anticipate major changes between the Release Candidate and Final Release versions of Windows XP SP2, it cannot absolutely guarantee the effectiveness of this procedure on a Final Release version of Windows XP SP2.

Cyberlogic Technologies, Inc., is committed to customer satisfaction. Please, send questions or comments to Cyberlogic's Technical Support (techsupport@cyberlogic.com).

ETHERNET MBX DRIVER

The following section describes a simple method to correct the compatibility issues that have arisen between the *Ethernet MBX Driver* and *Windows XP SP2 (RC2)*. To correct compatibility issues between the *Remote MBX Driver* and *Windows XP SP2 (RC2)* between two WinXP SP2 systems, refer to WinXP SP2 to WinXP SP2. Likewise, refer to WinXP SP2 to Win2000 SP4 to correct compatibility issues between the *Remote MBX Driver* and *Windows XP SP2 (RC2)* between WinXP SP2 and non-WinXP SP2 systems.

Problem Description

In keeping with Microsoft's goal of improved default network security configurations, *Windows XP SP2 (RC2)* closes most ports by default with *Windows Firewall*. Windows Firewall – aside from a few exceptions – blocks all unsolicited incoming communications through TCP/IP.

This functionality impedes the *Ethernet MBX Driver's* ability to handle unsolicited communications over TCP/IP. Unsolicited communications sent to a Windows XP SP2 (RC2) system over TCP/IP are blocked by Windows Firewall.

To learn more about Windows Firewall, visit Microsoft's Changes to Functionality in Windows XP SP2 (Windows Firewall) (http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx#XSLTsection130121120120) document.

Compatibility Solution

The following solution configures *Windows Firewall* to open Port *502*. By default, Windows Firewall closes this port. However, it must be open for unsolicited communications over Modbus TCP/IP to function.

1. Double-click *Windows Security Center* within Control Panel. Click *Windows Firewall* toward the bottom of the screen.

Figure 1: Windows Security Center.

2. Verify *Windows Firewall* is On.

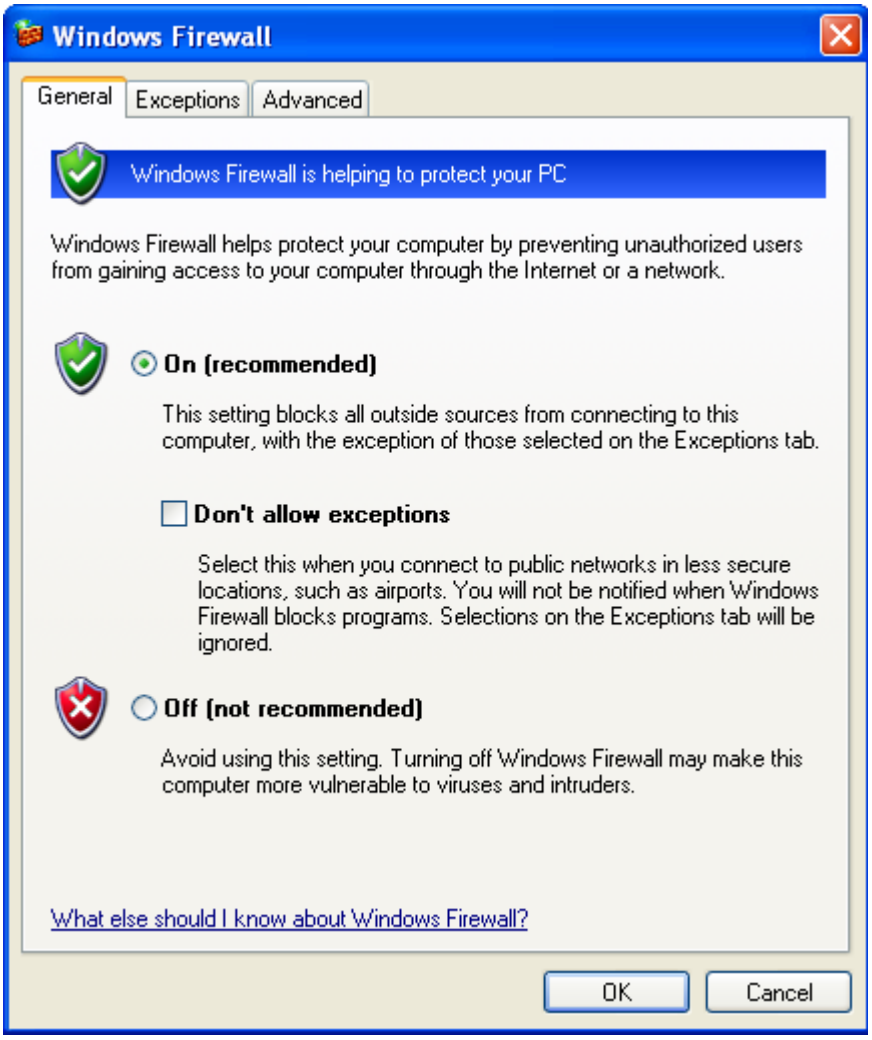

Figure 2: Windows Firewall (General Tab).

3. Select the *Exceptions* tab. Click *Add Port…*

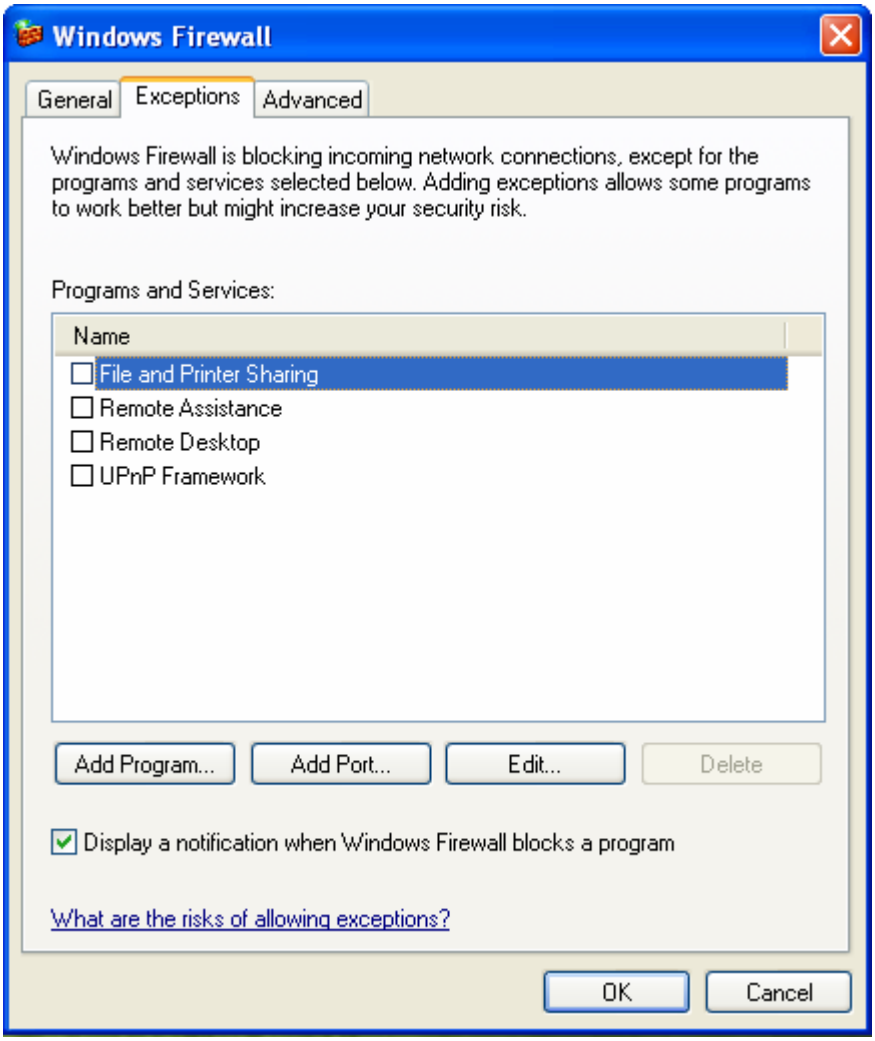

Figure 3: Windows Firewall (Exceptions Tab).

4. Type *Modbus TCP/IP* in the Name textbox and *502* in the Port Number textbox. Verify the *TCP* radio is selected. Click *Ok*.

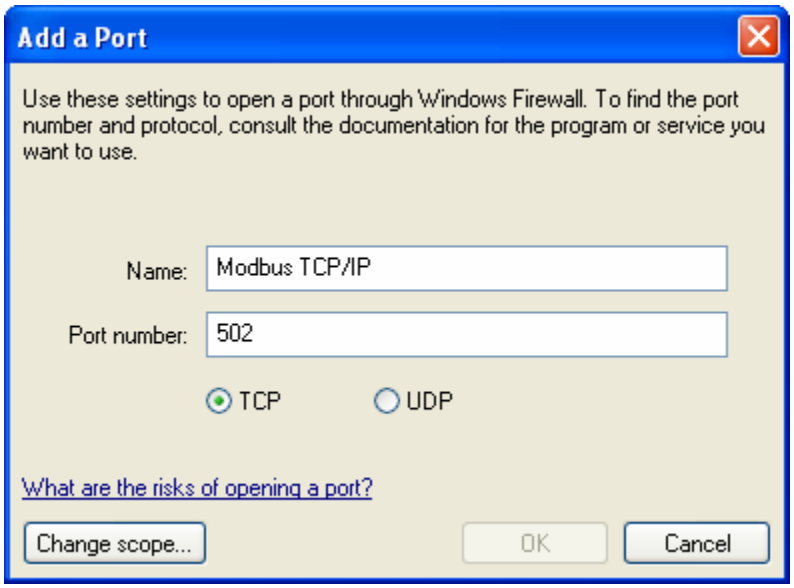

Figure 4: Add a Port Screen.

5. Verify the *Modbus TCP/IP* selection is checked. Click *Ok*.

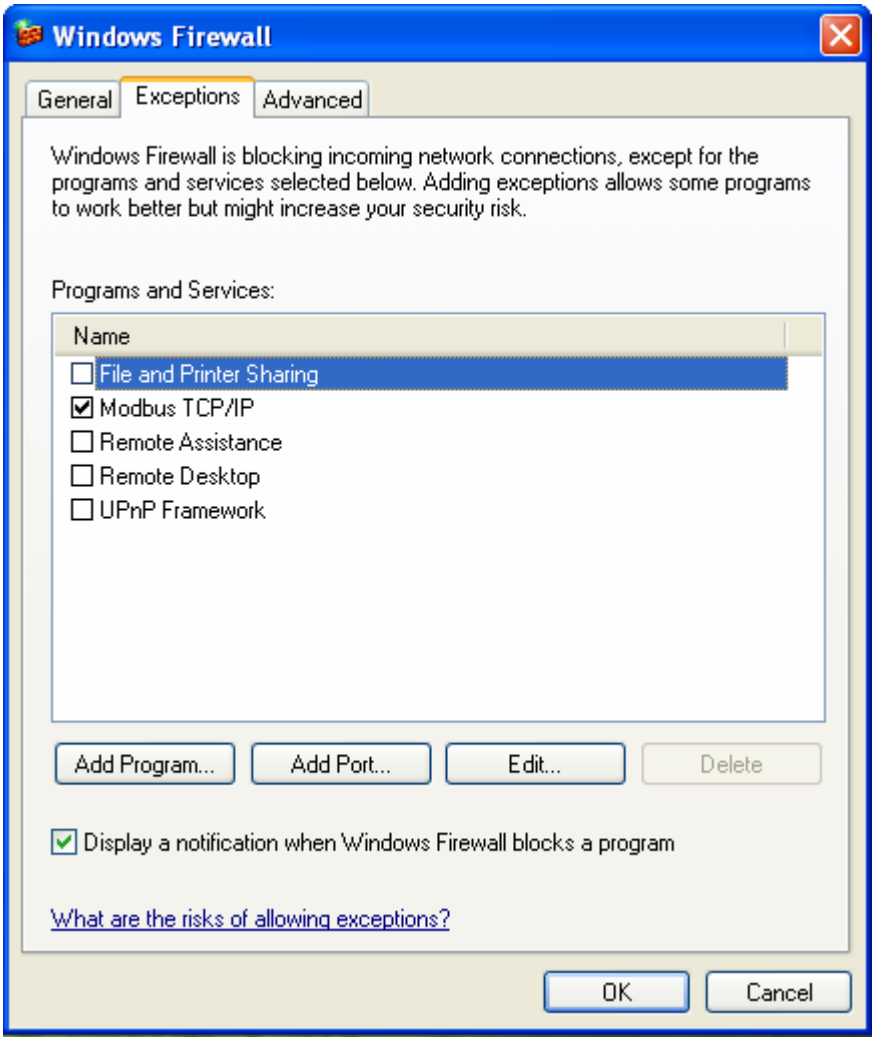

Figure 5: Windows Firewall (Exceptions Tab) with Modbus TCP/IP Exception.

6. Repeat this procedure for any *Windows XP SP2* system that may receive unsolicited communications over Modbus TCP/IP.

REMOTE MBX DRIVER

The following section describes a simple method to correct the compatibility issues that have arisen between the *Remote MBX Driver* and *Windows XP SP2 (RC2)*. Refer to WinXP SP2 to WinXP SP2 to correct compatibility issues between two WinXP SP2 systems. Likewise, refer to WinXP SP2 to Win2000 SP4 to correct compatibility issues between WinXP SP2 and non-WinXP SP2 systems. To correct compatibility issues between the *Ethernet MBX Driver* and *Windows XP SP2 (RC2)*, refer to Ethernet MBX Driver.

WinXP SP2 to WinXP SP2

The following section describes a simple method to correct the compatibility issues that have arisen between the *Remote MBX Driver* and *Windows XP SP2 (RC2)* between two WinXP SP2 systems. This section applies both to systems that contain an MBX Remote Server and those that contain an MBX Remote Client.

Problem Description

In keeping with Microsoft's goal of improved default network security configurations, *Windows XP SP2 (RC2)* closes most ports by default with *Windows Firewall*. Windows Firewall – aside from a few exceptions – blocks all unsolicited incoming communications through TCP/IP. In addition, communications between two systems along a local network are impossible without configuring the local network.

This functionality impedes the *Remote MBX Driver's* ability to handle communications between an MBX Remote Server and MBX Remote Client. Without configuring a local network, information cannot be sent between two systems – even if they seem to reside on the same network. In addition, Windows Firewall blocks communications between MBX Remote Servers and MBX Remote Clients operating on Windows XP SP2 systems.

To learn more about Windows Firewall, visit Microsoft's Changes to Functionality in Windows XP SP2 (Windows Firewall) (http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx#XSLTsection130121120120) document.

Compatibility Solution

The following solution configures a local network and forces *Windows Firewall* to allow File and Printer Sharing. By default, systems that reside on a network are not allowed to communicate with one another before a network is configured. However, such systems must communicate with one another for the *MBX Remote Driver* to function. Furthermore, ports *137* through *139* – which are necessary for File and Printer Sharing – must be open for communications between an MBX Remote Server and MBX Remote Client to function.

To determine whether or not two Windows XP SP2 systems may communicate with one another over a local network, open *Windows Explorer* and access a system through *My Network Places*. If a Login window appears, the systems may not communicate.

Users must perform the following procedure on both Windows XP SP2 systems.

1. Double-click *Network Connections* within Control Panel. Click *Set Up a Home or Small Office Network*.

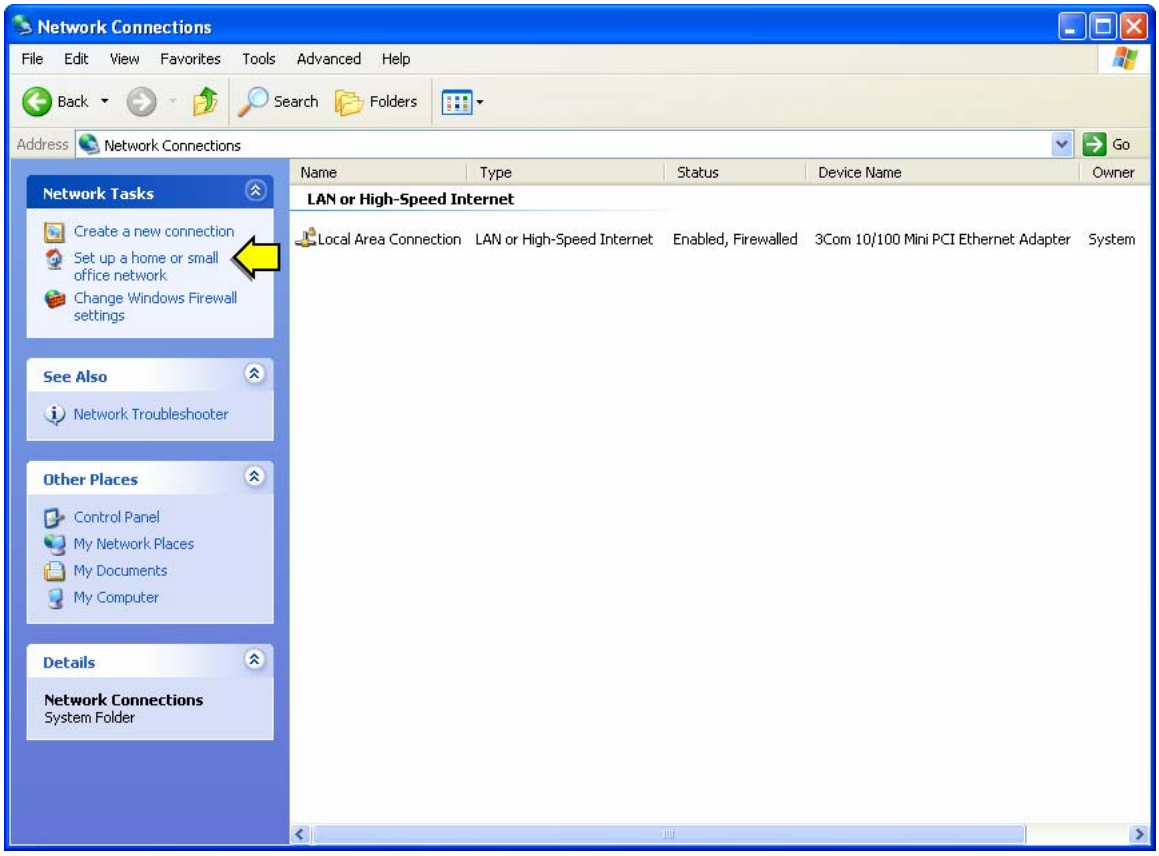

Figure 6: Network Connections Screen.

2. Click *Next*.

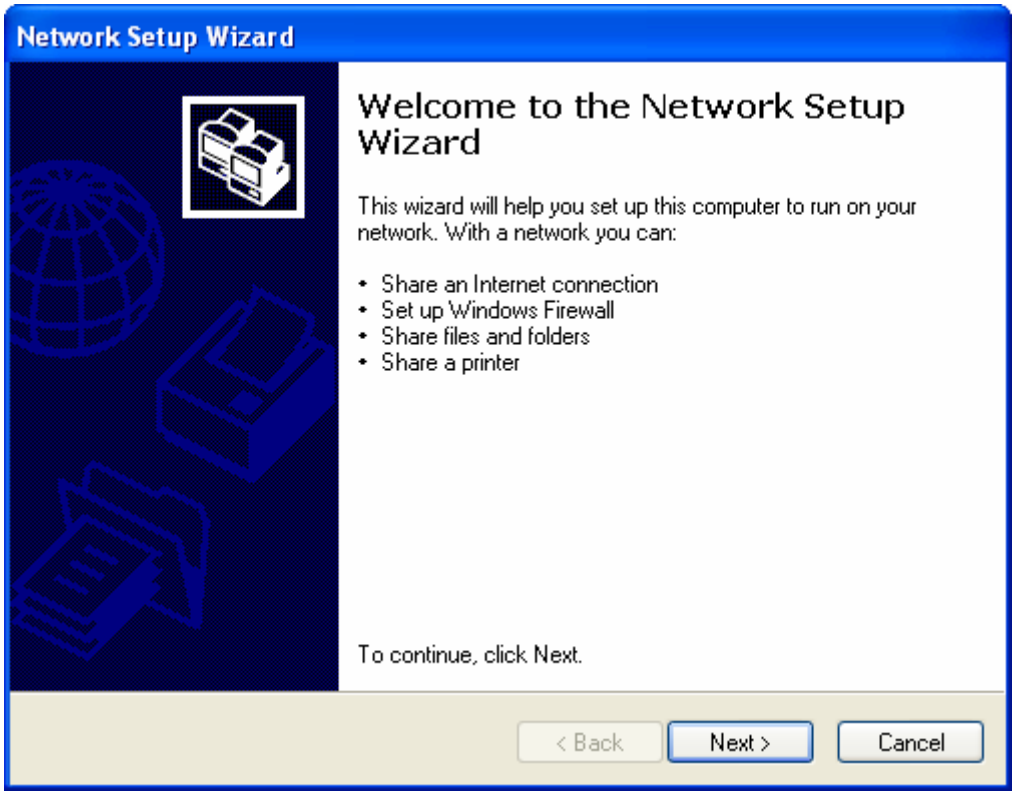

Figure 7: Network Configuration Wizard.

3. Click *Next*.

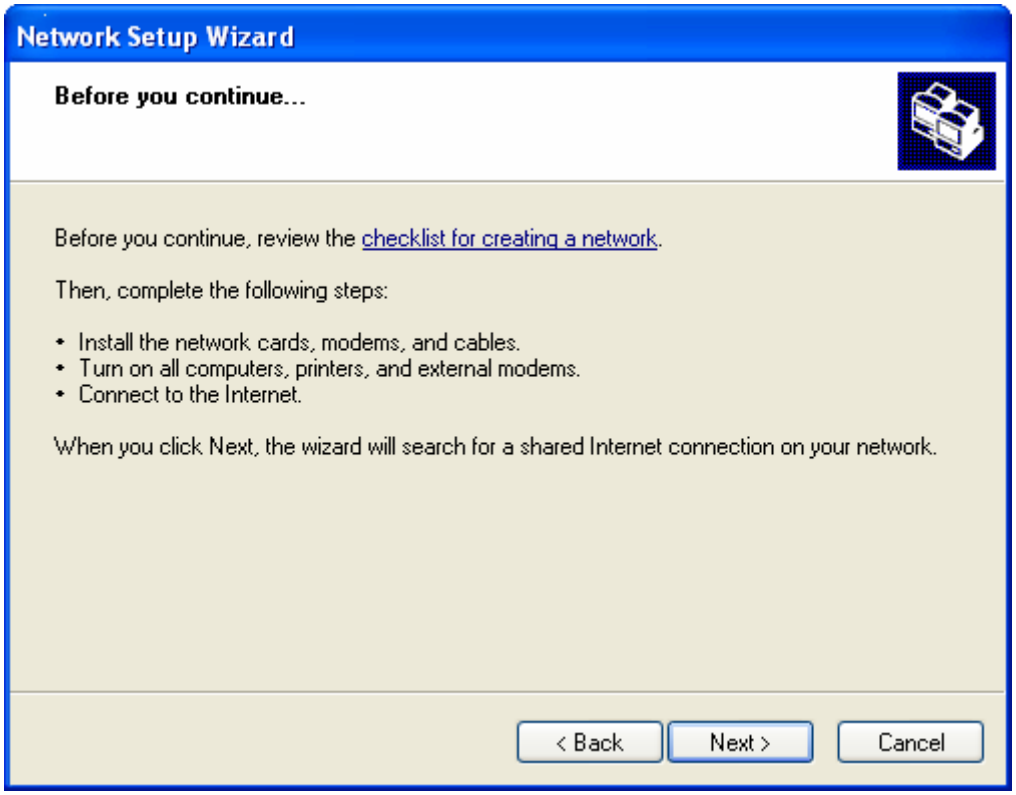

Figure 8: Network Configuration Screen.

4. Be sure the *This Computer Connects to the Internet through a Residential Gateway or …* radio is selected. Click *Next*.

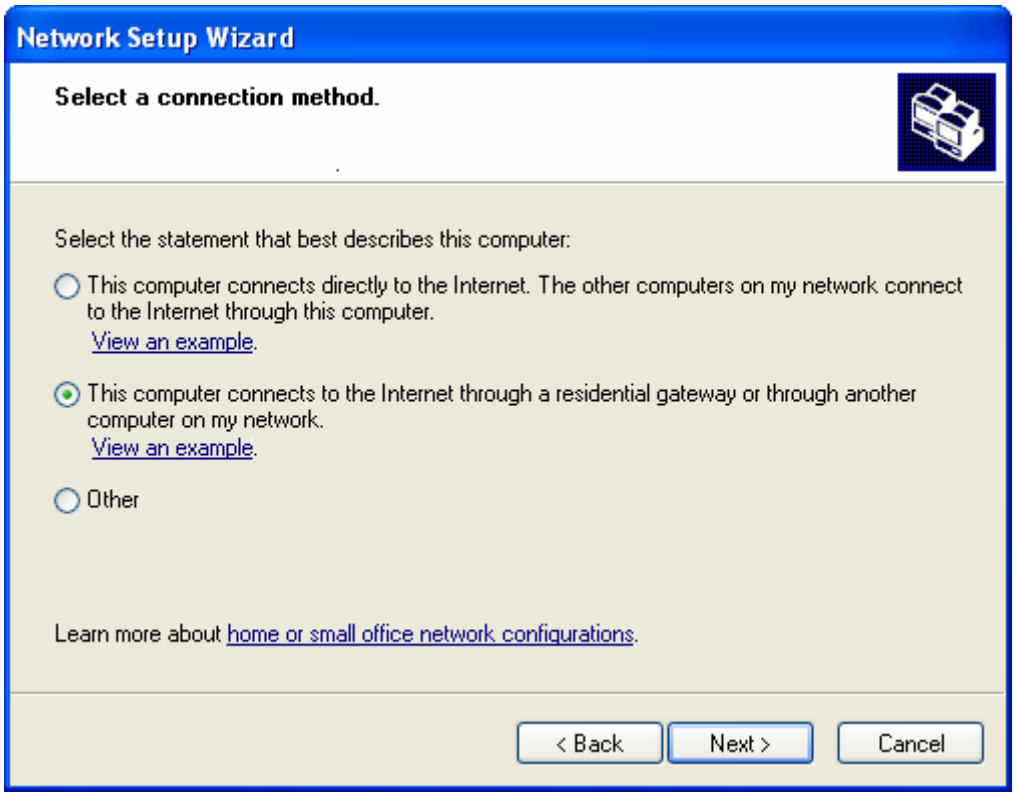

Figure 9: Network Configuration Screen.

5. Provide a Computer Description and Computer Name to identify your system on the local network. In this example, Computer Description is *Compatibility Solution* and Computer Name is *CYBERLOGIC*. Click *Next.*

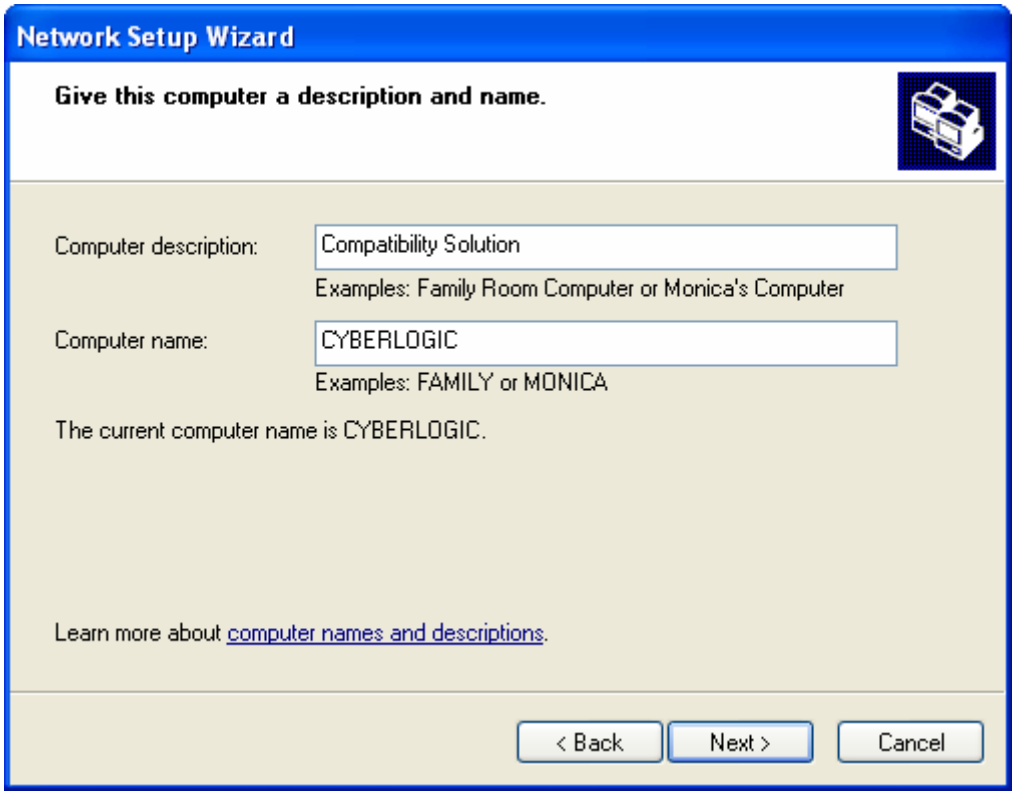

Figure 10: Network Configuration Screen.

6. Provide a Workgroup Name to identify the network upon which your network resides. In this example, Workgroup Name is *WORKGROUP*. Click *Next.*

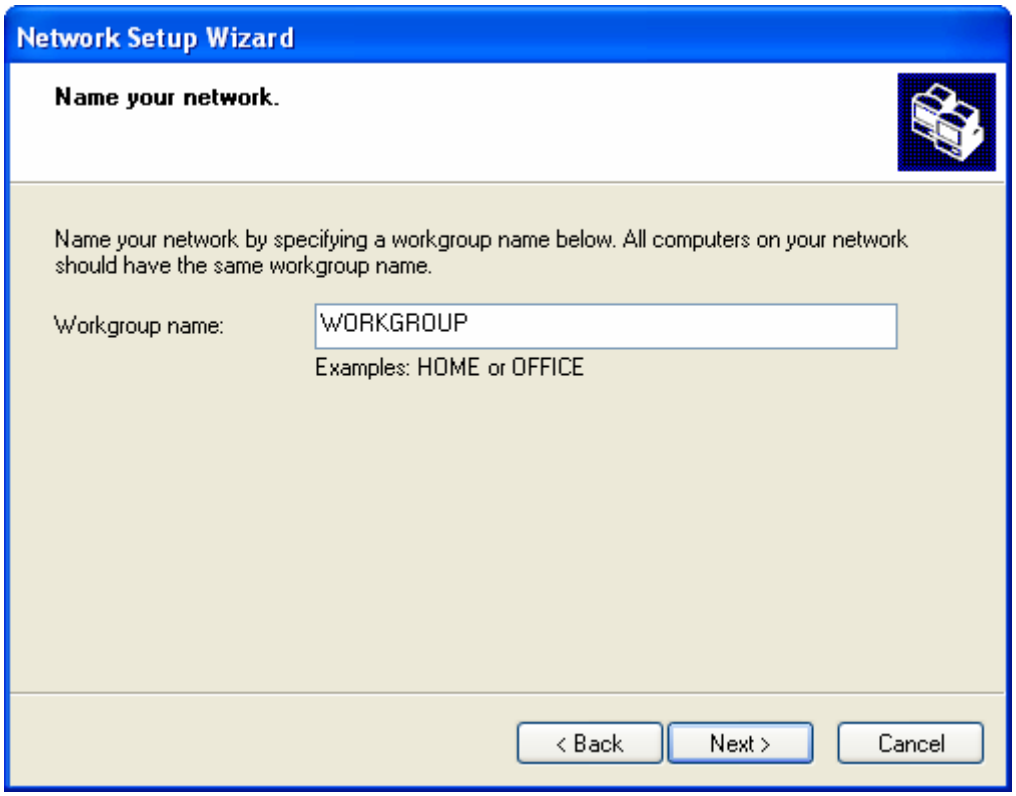

Figure 11: Network Configuration Screen.

7. Be sure the *Turn Off File and Printer Sharing* radio is selected. Click *Next.*

Note: Normally, the user may select the *Turn On File and Printer Sharing* radio. However, this document will describe the process by which a user may allow File and Printer Sharing through the *Windows Security Center*. If the user wishes to skip this explanation – or already knows the procedure by which he may allow File and Printer Sharing through the Windows Security Center – he may select the *Turn On File and Printer Sharing* radio.

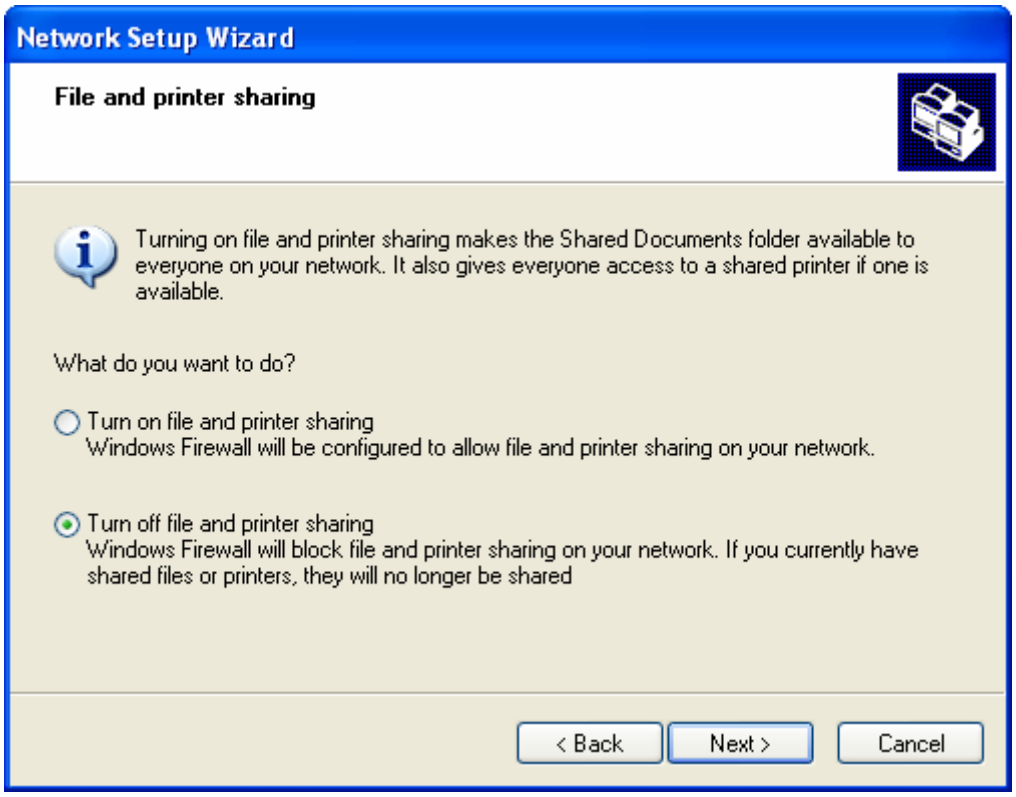

Figure 12: Network Configuration Screen.

8. Click *Next*.

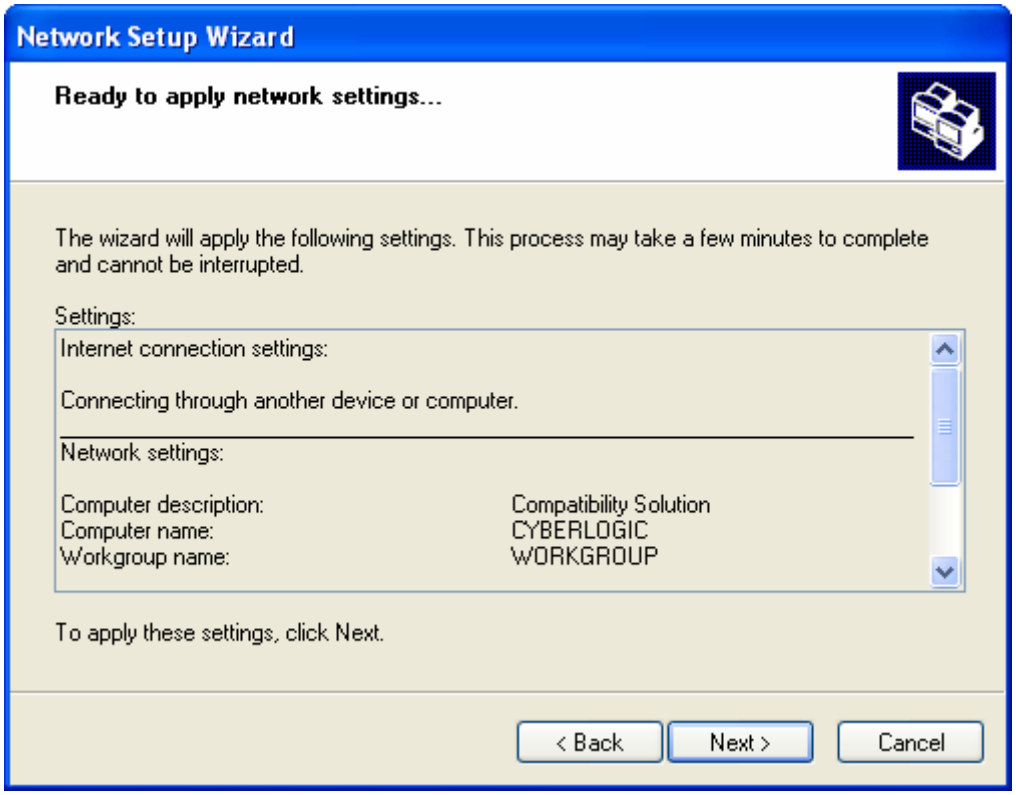

Figure 13: Network Configuration Screen.

9. Select the *Just Finish …* radio. Click *Next*.

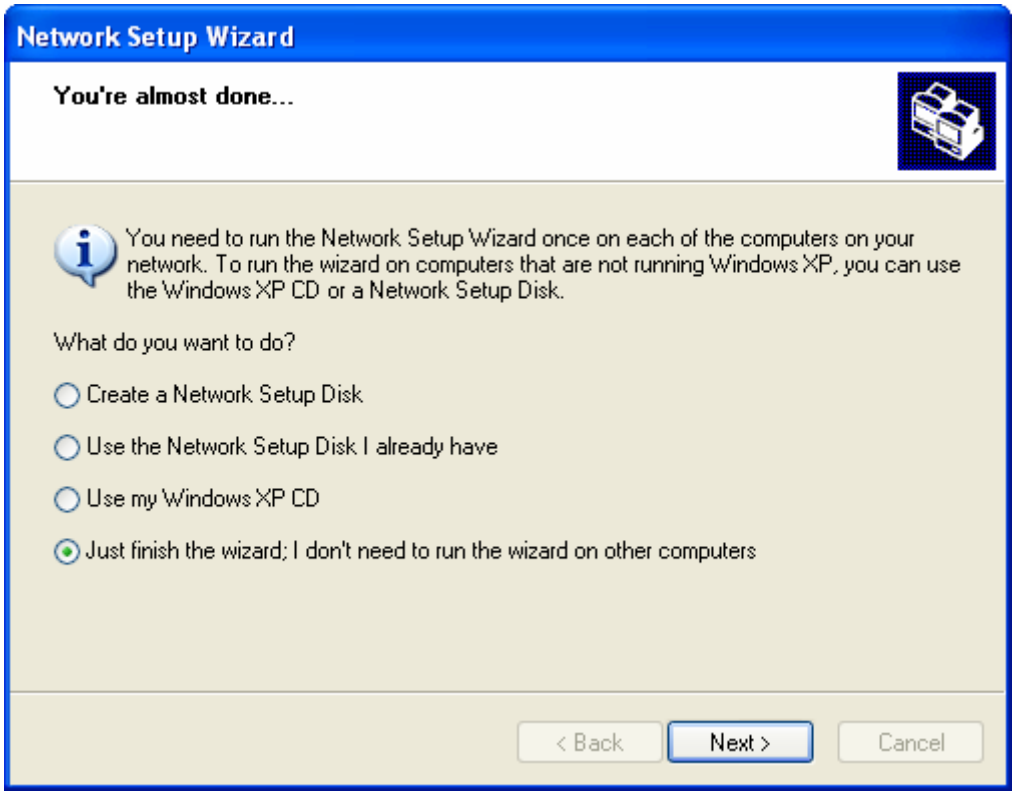

Figure 14: Network Configuration Screen.

10. Click *Finish*.

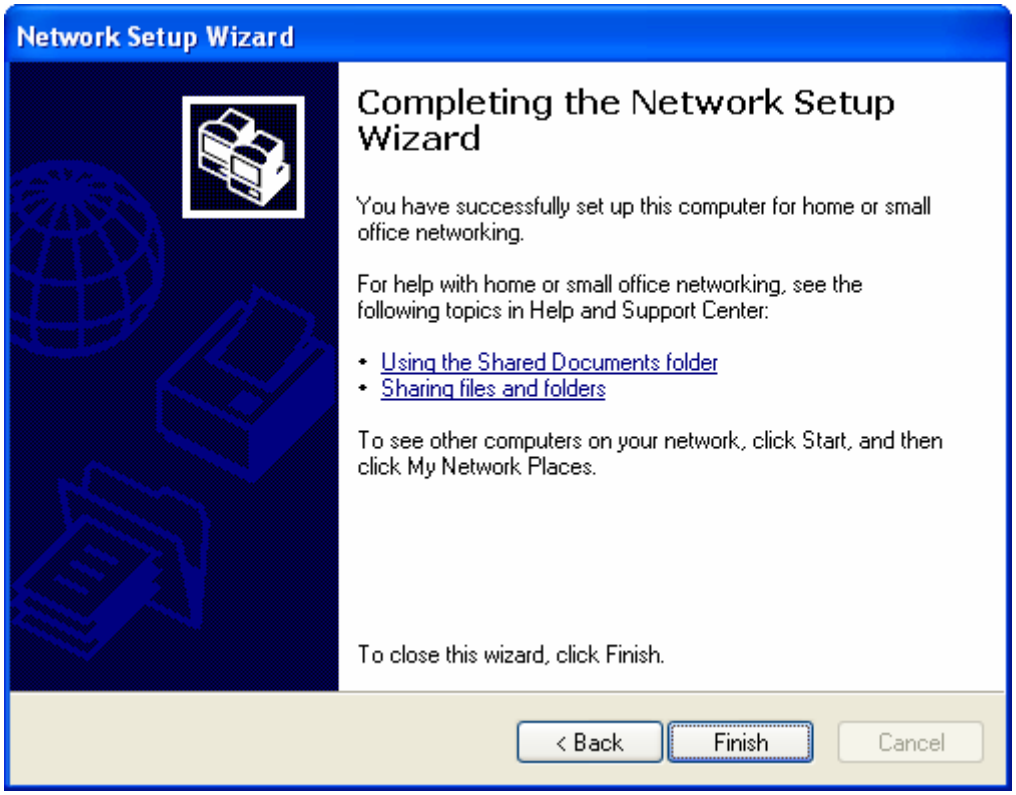

Figure 15: Network Configuration Screen.

11. The following steps describe the process by which a user may allow File and Printer Sharing through the Windows Security Center. If the user selected the *Turn On File and Printer Sharing* radio in the 7th step of this procedure, he may proceed to the 14th step.

    Double-click *Windows Security Center* within Control Panel. Click *Windows Firewall* toward the bottom of the screen.

Figure 16: Windows Security Center.

12. Verify *Windows Firewall* is On.

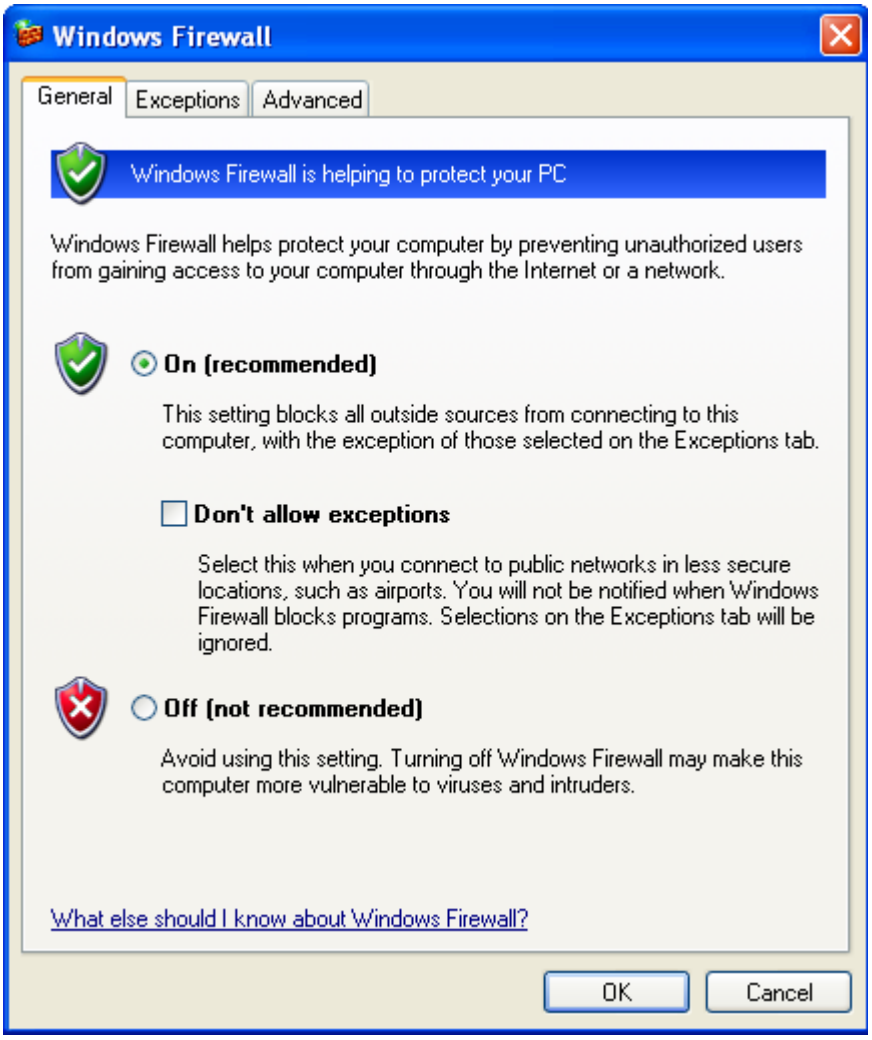

Figure 17: Windows Firewall (General Tab).

13. Select the *Exceptions* tab. Activate the *File and Printer Sharing* checkbox. Click *Ok*.

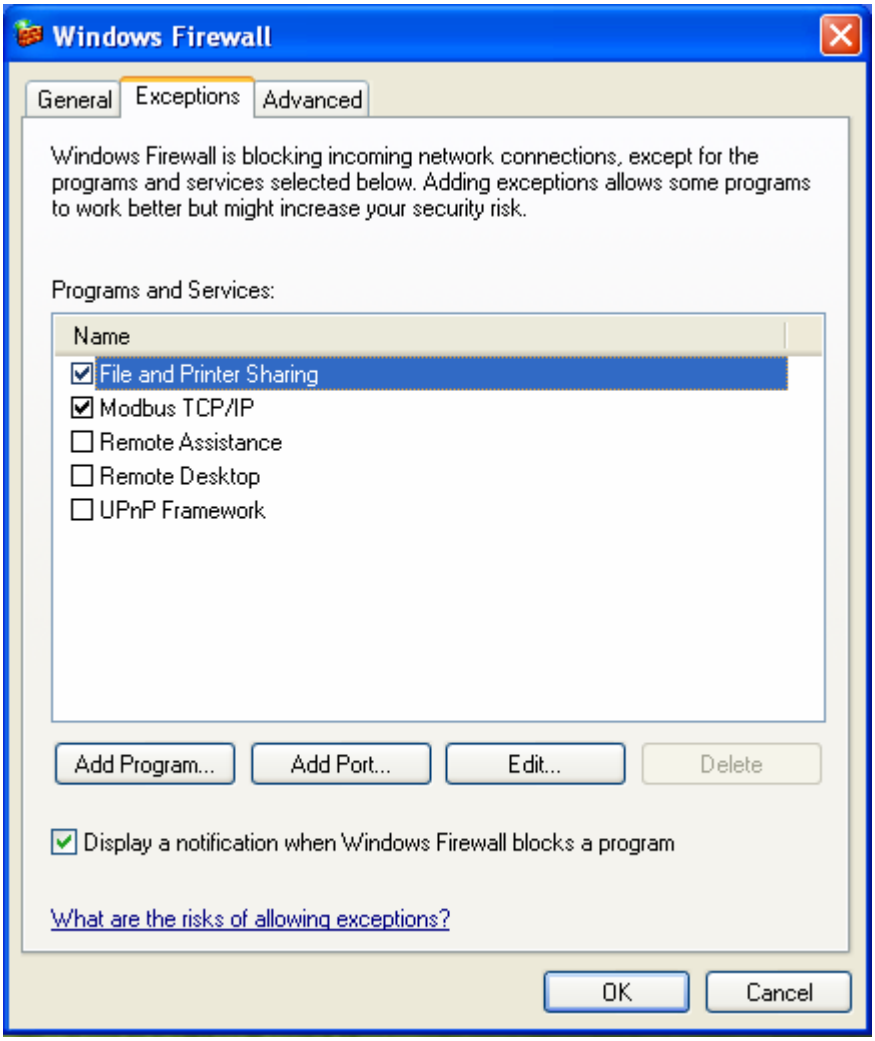

Figure 18: Windows Firewall (Exceptions Tab).

14. Repeat this procedure for any other Windows XP SP2 systems that may communicate using the *Remote MBX Driver*.

WinXP SP2 to Win2000 SP4

The following section describes a simple method to correct the compatibility issues that have arisen between the *Remote MBX Driver* and *Windows XP SP2 (RC2)* between WinXP SP2 and non-WinXP SP2 systems. In this procedure, the non-WinXP SP2 system contains the *Windows 2000 SP4* operating system.

Note: Cyberlogic only guarantees the effectiveness of the following procedure for Windows 2000 SP4.

This section applies both to systems that contain an MBX Remote Server and those that contain an MBX Remote Client. That is, the procedure is identical whether the MBX Remote Server resides on the Win2000 system and the MBX Remote Client resides on the WinXP system, or the MBX Remote Server resides on the WinXP system and the MBX Remote Client resides on the Win2000 system.

Problem Description

In keeping with Microsoft's goal of improved default network security configurations, *Windows XP SP2 (RC2)* closes most ports by default with *Windows Firewall*. Windows Firewall – aside from a few exceptions – blocks all unsolicited incoming communications through TCP/IP. In addition, communications between two systems along a local network are impossible without configuring the local network.

This functionality impedes the *Remote MBX Driver's* ability to handle communications between an MBX Remote Server and MBX Remote Client. Without configuring a local network, information cannot be sent between two systems – even if they seem to reside on the same network. In addition, Windows Firewall blocks communications between MBX Remote Servers and MBX Remote Clients operating on Windows XP SP2 systems.

To learn more about Windows Firewall, visit Microsoft's Changes to Functionality in Windows XP SP2 (Windows Firewall) (http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx#XSLTsection130121120120) document.

Compatibility Solution

The following solution configures a local network and forces *Windows Firewall* to allow File and Printer Sharing. By default, systems that reside on a network are not allowed to communicate with one another before a network is configured. However, such systems must communicate with one another for the *MBX Remote Driver* to function. Furthermore, ports *137* through *139* – which are necessary for File and Printer Sharing – must be open for communications between an MBX Remote Server and MBX Remote Client to function.

To determine whether or not a *WinXP SP2* system may communicate with a *Win2000 SP4* system over a local network, open *Windows Explorer* on both systems and access the other computer through *My Network Places*. If a Login window appears on either system, the systems may not communicate.

This procedure begins by configuring the Windows XP SP2 system.

Windows XP SP2 System

1. Double-click *Network Connections* within Control Panel. Click *Set Up a Home or Small Office Network*.

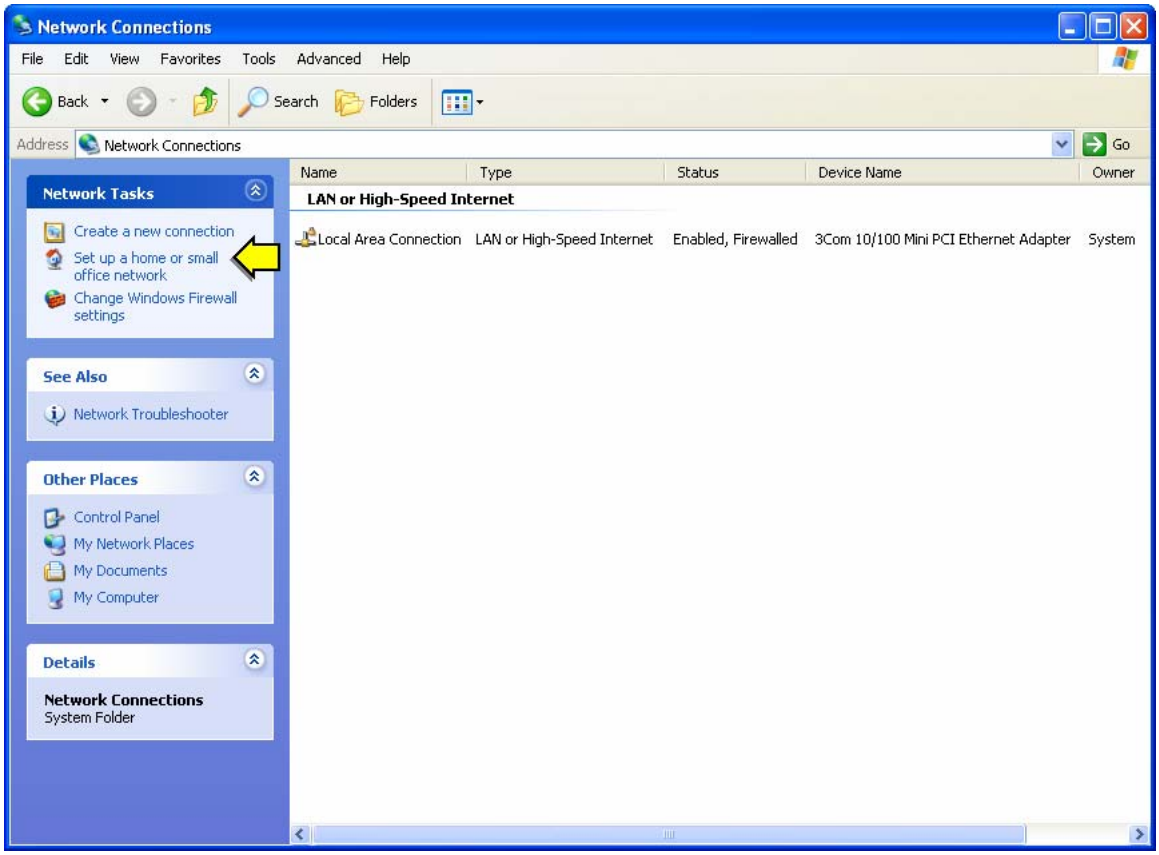

Figure 19: Network Connections Screen.

2. Click *Next*.

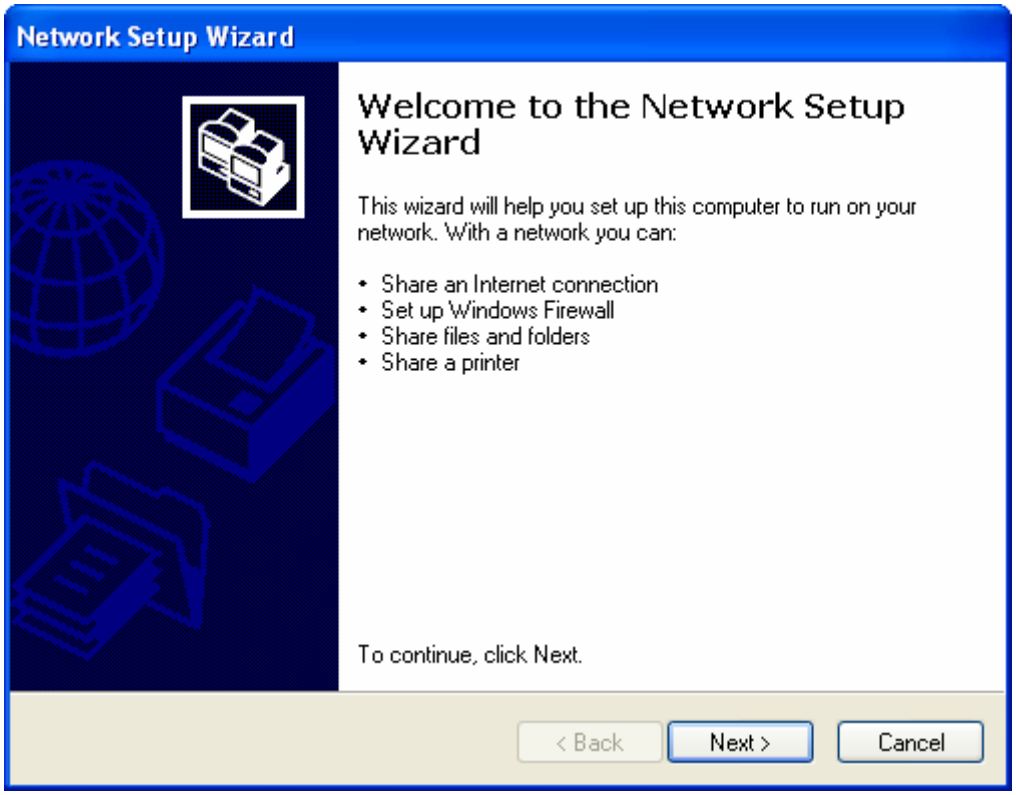

Figure 20: Network Configuration Wizard.

3. Click *Next*.

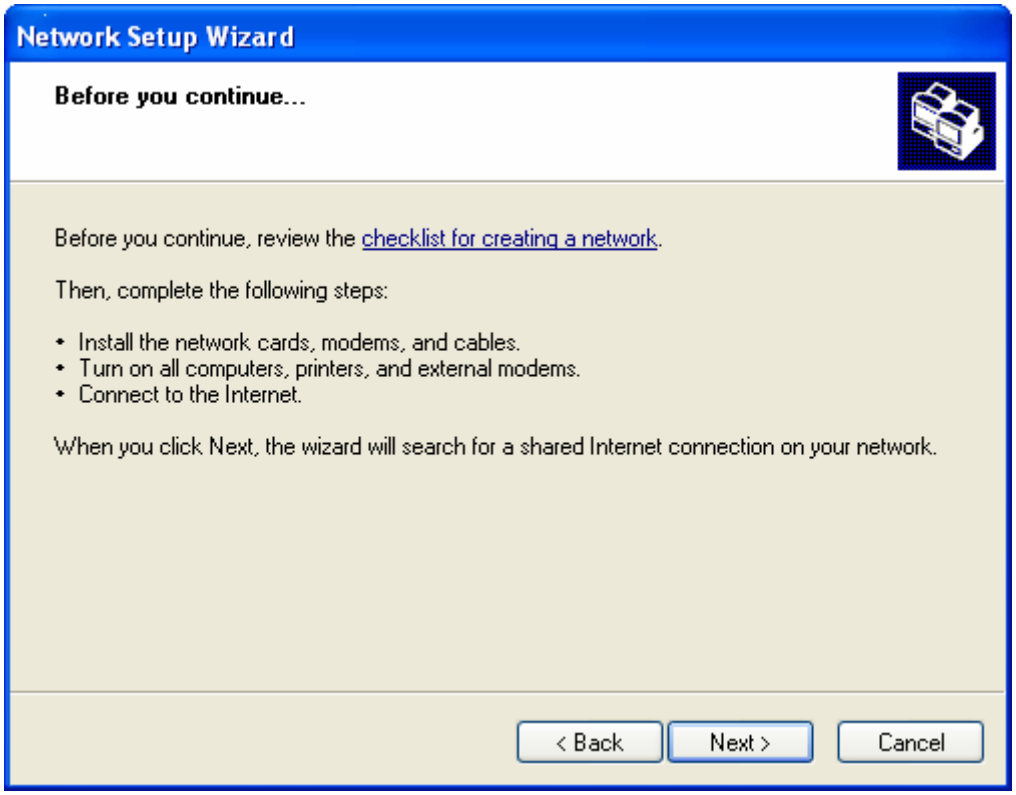

Figure 21: Network Configuration Screen.

4. Be sure the *This Computer Connects to the Internet through a Residential Gateway or …* radio is selected. Click *Next*.

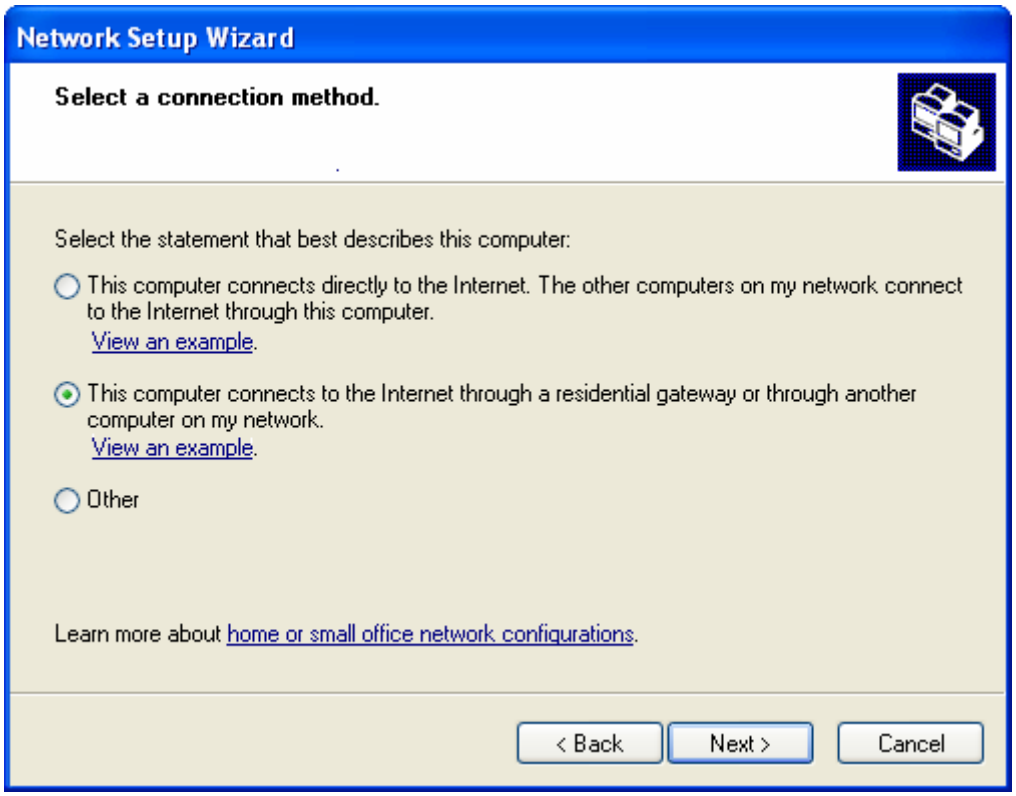

Figure 22: Network Configuration Screen.

5. Provide a Computer Description and Computer Name to identify your system on the local network. In this example, Computer Description is *Compatibility Solution* and Computer Name is *CYBERLOGIC*.

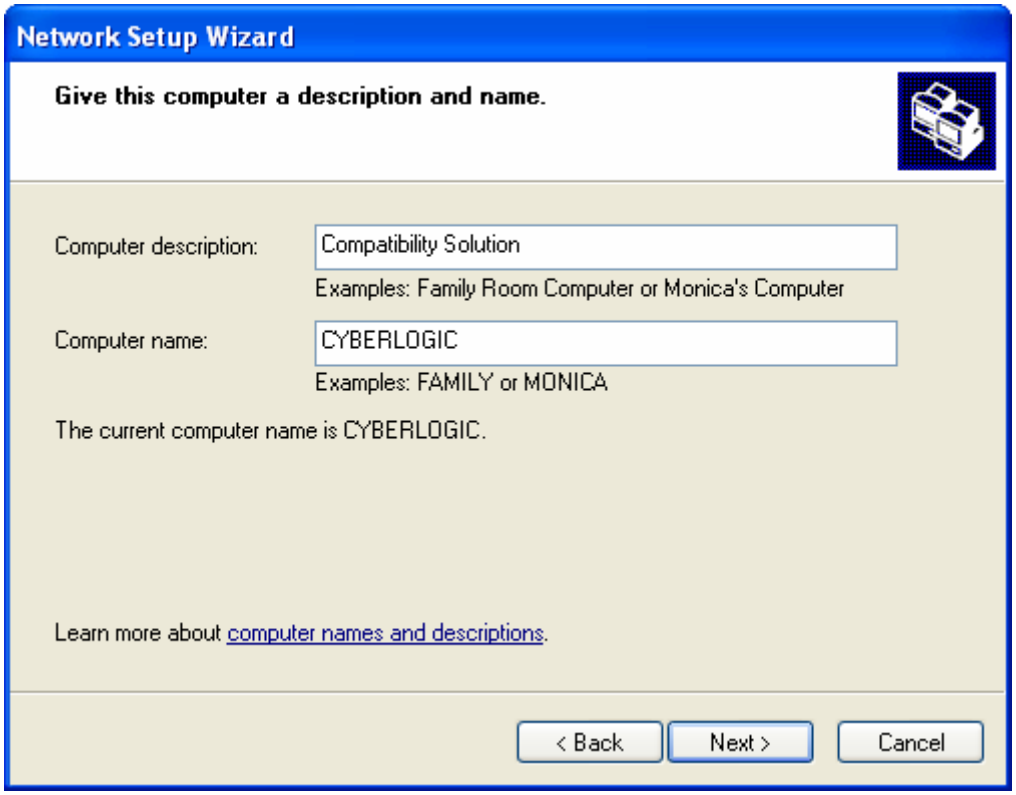

Figure 23: Network Configuration Screen.

6. Provide a Workgroup Name to identify the network upon which your network resides. In this example, Workgroup Name is *WORKGROUP*.

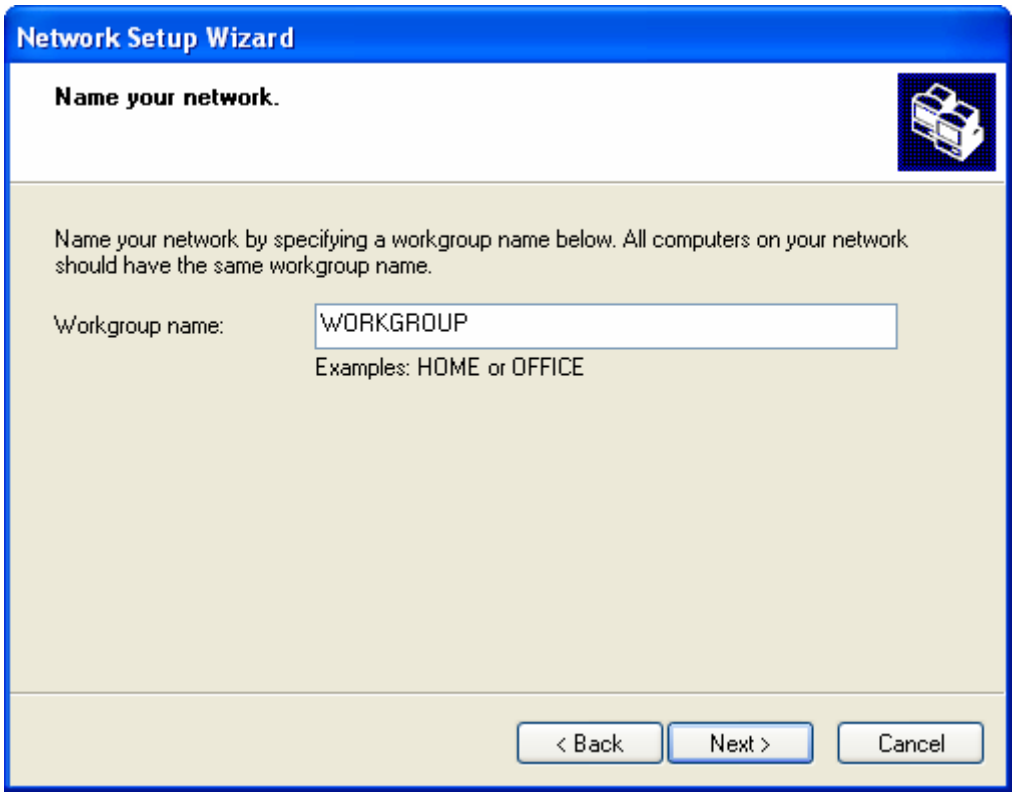

Figure 24: Network Configuration Screen.

7. Be sure the *Turn Off File and Printer Sharing* radio is selected. Click *Next.*

Note: Normally, the user may select the *Turn On File and Printer Sharing* radio. However, this document will describe the process by which a user may allow File and Printer Sharing through the *Windows Security Center*. If the user wishes to skip this explanation – or already knows the procedure by which he may allow File and Printer Sharing through the Windows Security Center – he may select the *Turn On File and Printer Sharing* radio.

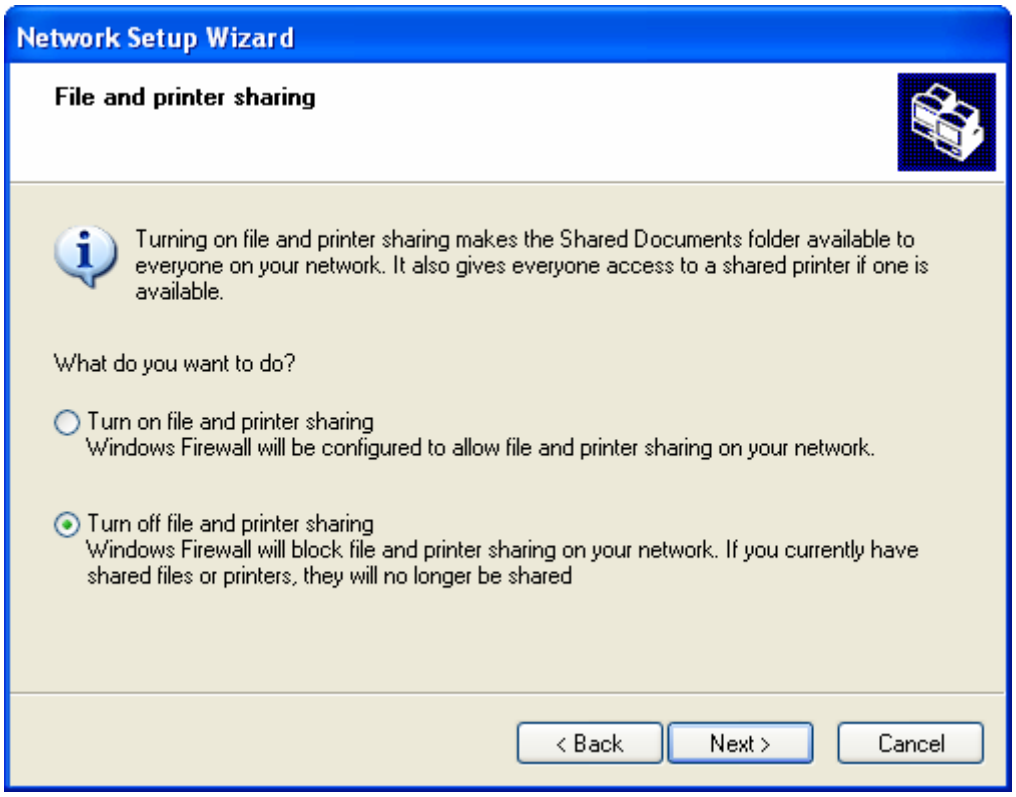

Figure 25: Network Configuration Screen.

8. Click *Next*.

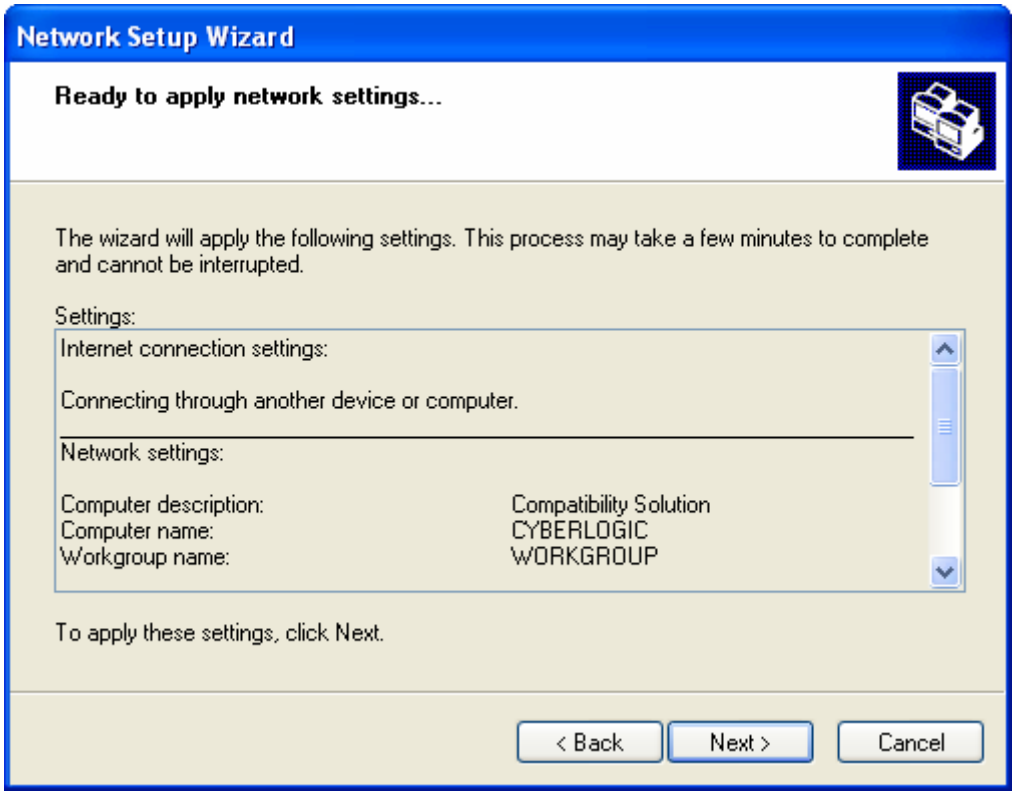

Figure 26: Network Configuration Screen.

9. Select the *Just Finish …* radio. Click *Next*.

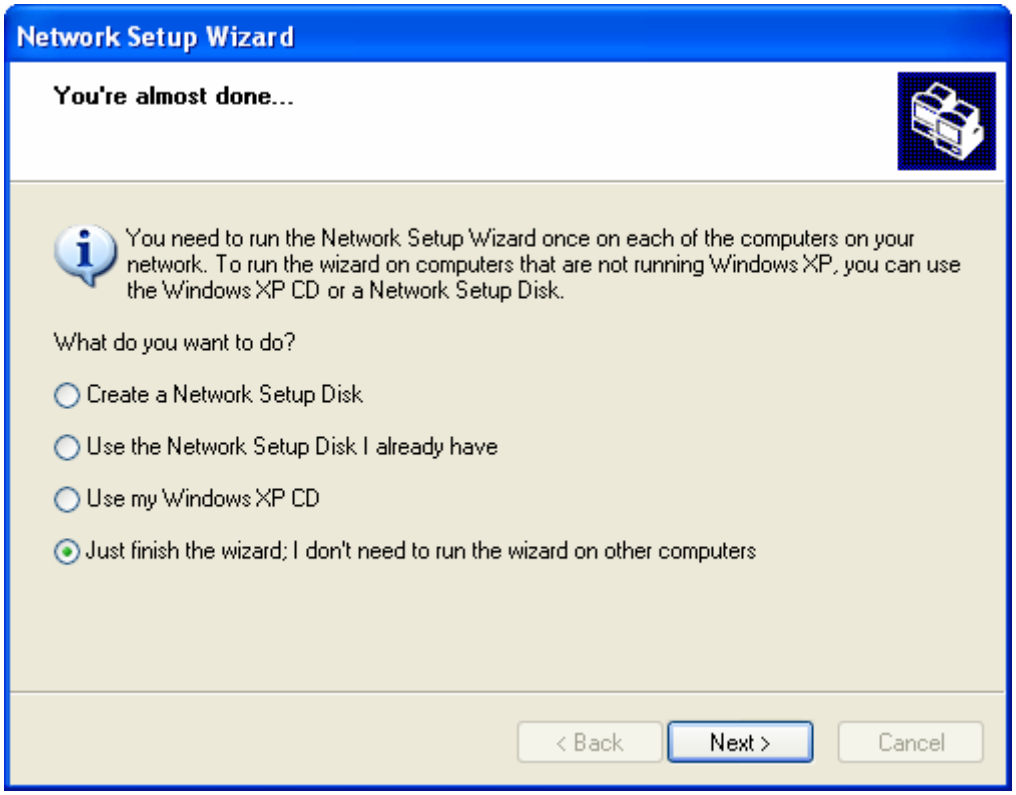

Figure 27: Network Configuration Screen.

10. Click *Finish*.

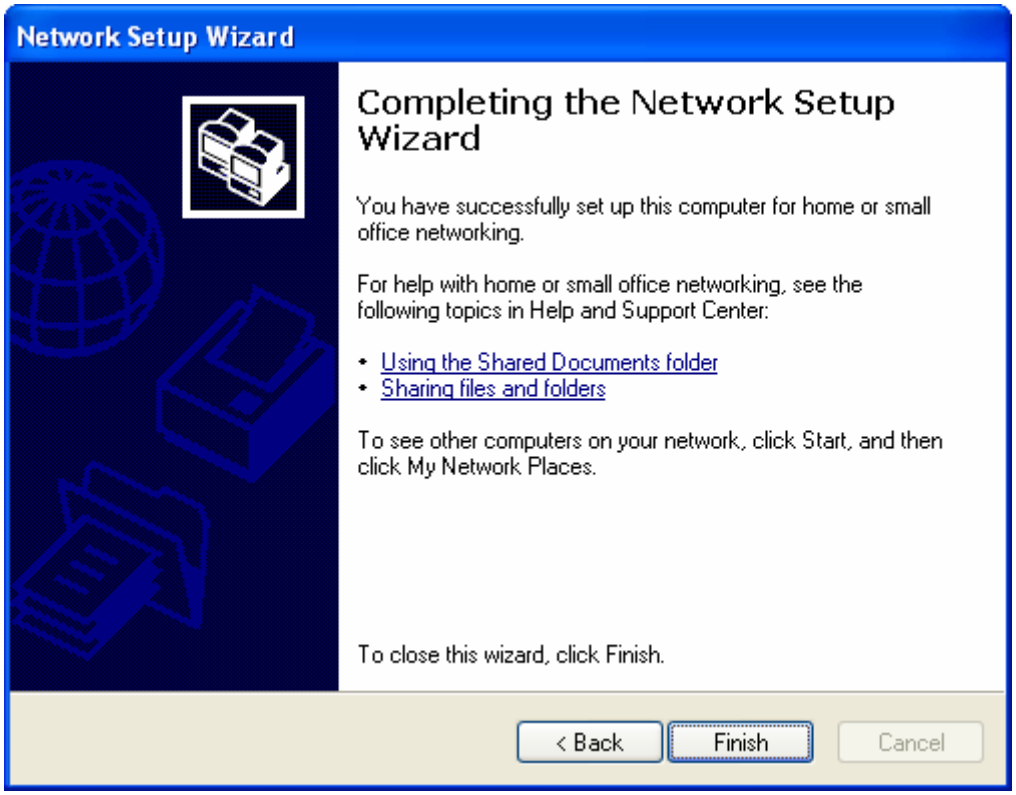

Figure 28: Network Configuration Screen.

11. The following steps describe the process by which a user may allow File and Printer Sharing through the Windows Security Center. If the user selected the *Turn On File and Printer Sharing* radio in the 7th step of this procedure, he may proceed to the 14th step.

    Double-click *Windows Security Center* within Control Panel. Click *Windows Firewall* toward the bottom of the screen.

Figure 29: Windows Security Center.

12. Verify *Windows Firewall* is On.

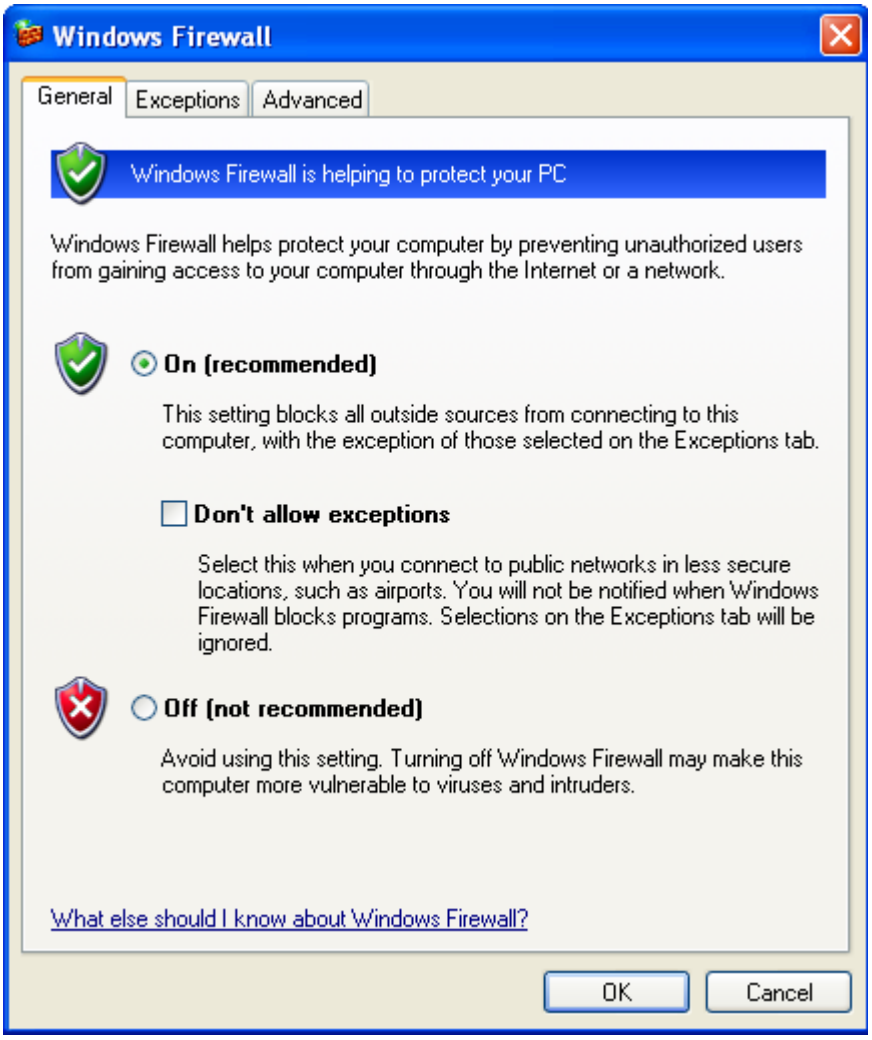

Figure 30: Windows Firewall (General Tab).

13. Select the *Exceptions* tab. Activate the *File and Printer Sharing* checkbox. Click *Ok*.

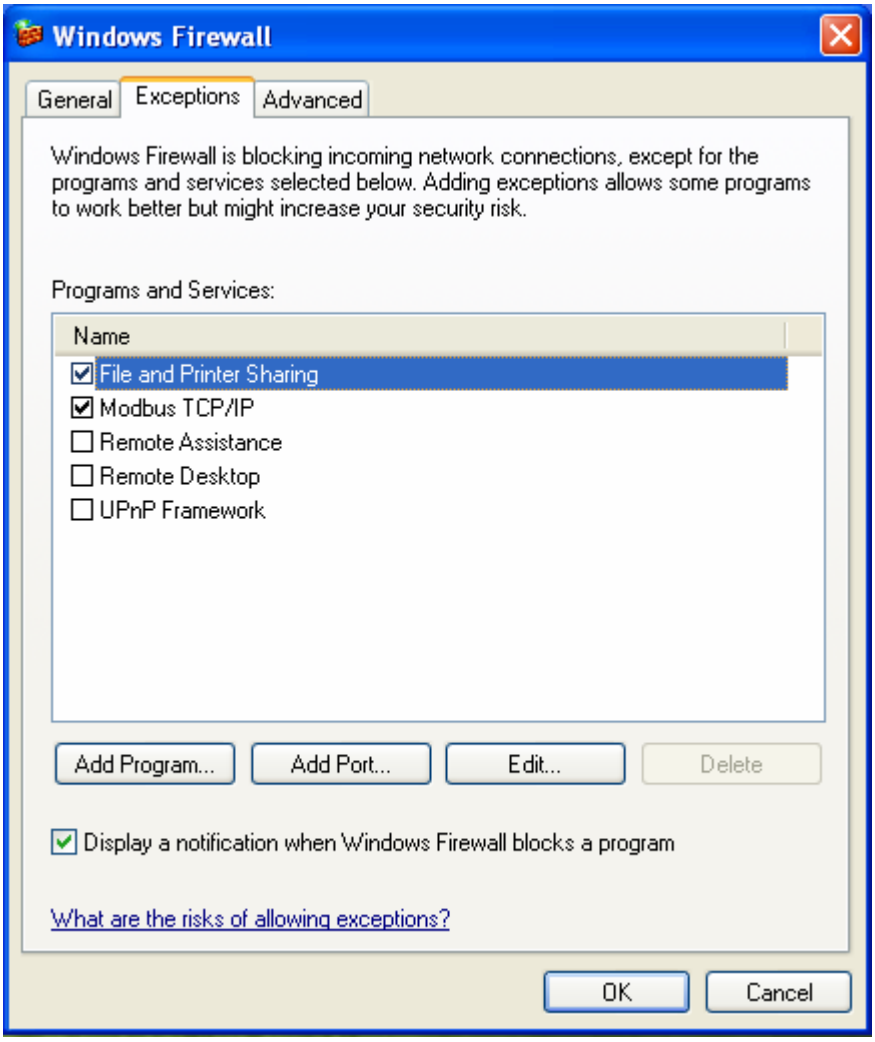

Figure 31: Windows Firewall (Exceptions Tab).

14. Repeat this procedure for any other Windows XP SP2 systems that may communicate using the *Remote MBX Driver*.

Windows 2000 SP4 System

15. This procedure continues by configuring the Windows 2000 SP4 system. The primary goal of this procedure is to allow access from other systems on the local network.

    Right-click *My Computer* and choose *Properties*. Select the *Network Identification* tab. Click *Network ID*.

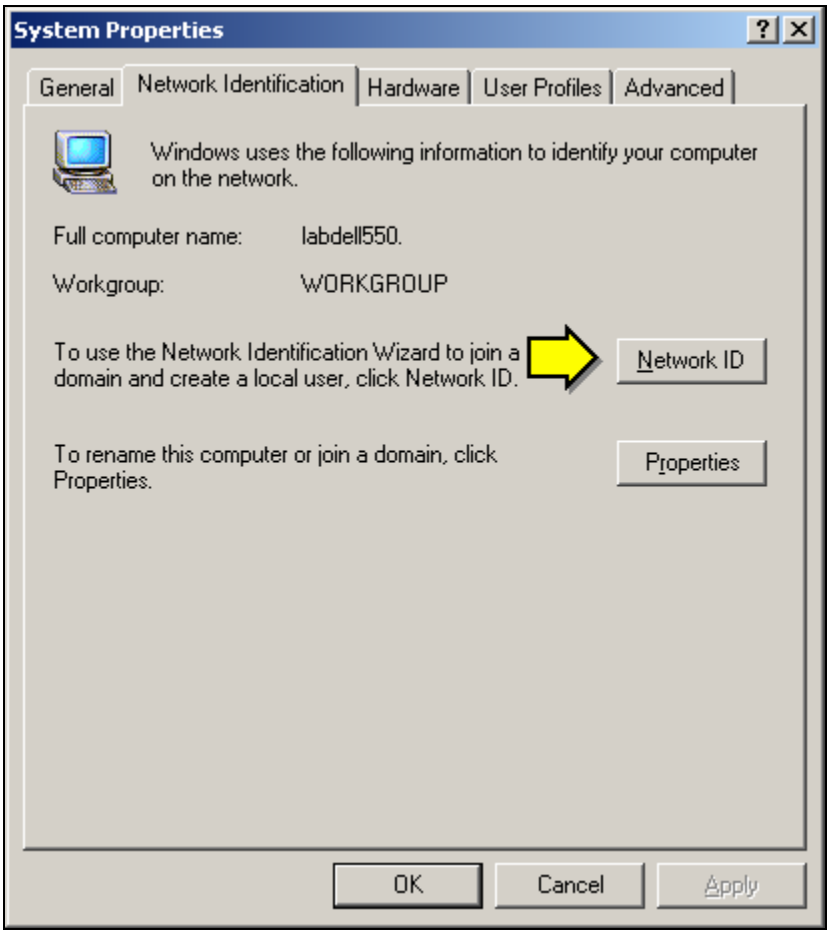

Figure 32: Network Identification Tab.

16. Click *Next.*

Figure 33: Network Identification Wizard Screen.

17. Select the *This Computer is Part of a Business Network …* radio. Click *Next*.

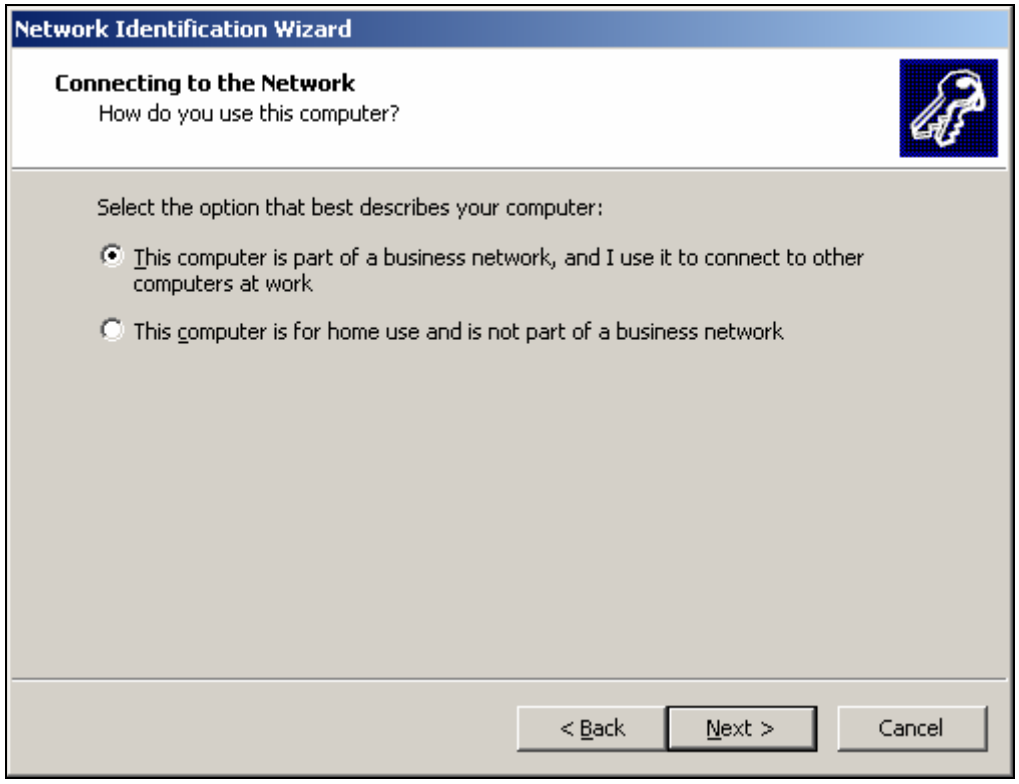

Figure 34: Network Identification Wizard Screen.

18. Select the *My Company Uses a Network Without a Domain* radio. Click *Next.*

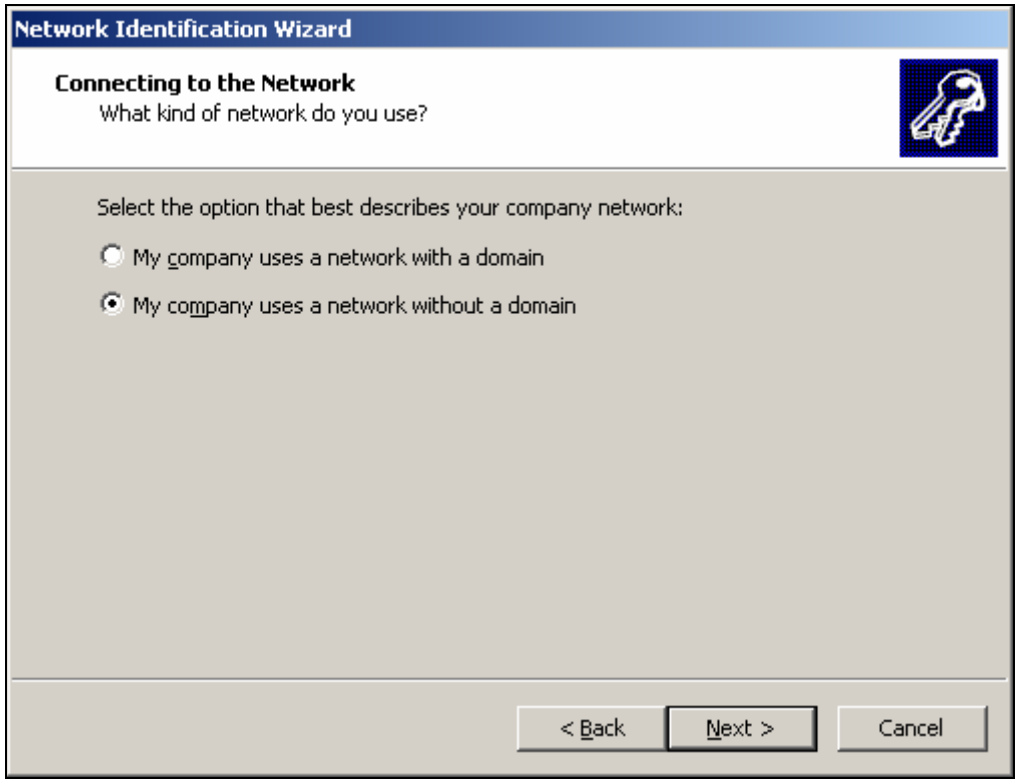

Figure 35: Network Identification Wizard Screen.

19. Provide a Workgroup Name to identify the network upon which your network resides. In this example, Workgroup Name is *WORKGROUP.* Click *Next*.

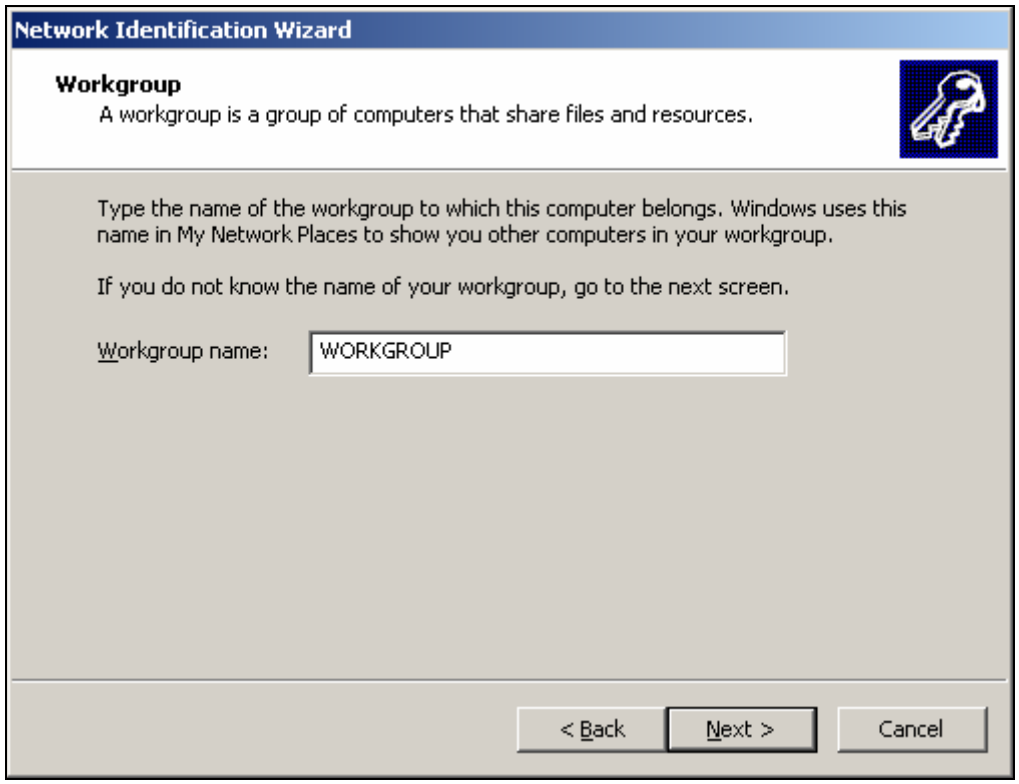

Figure 36: Network Identification Wizard Screen.

20. Click *Finish*. Reboot the system.

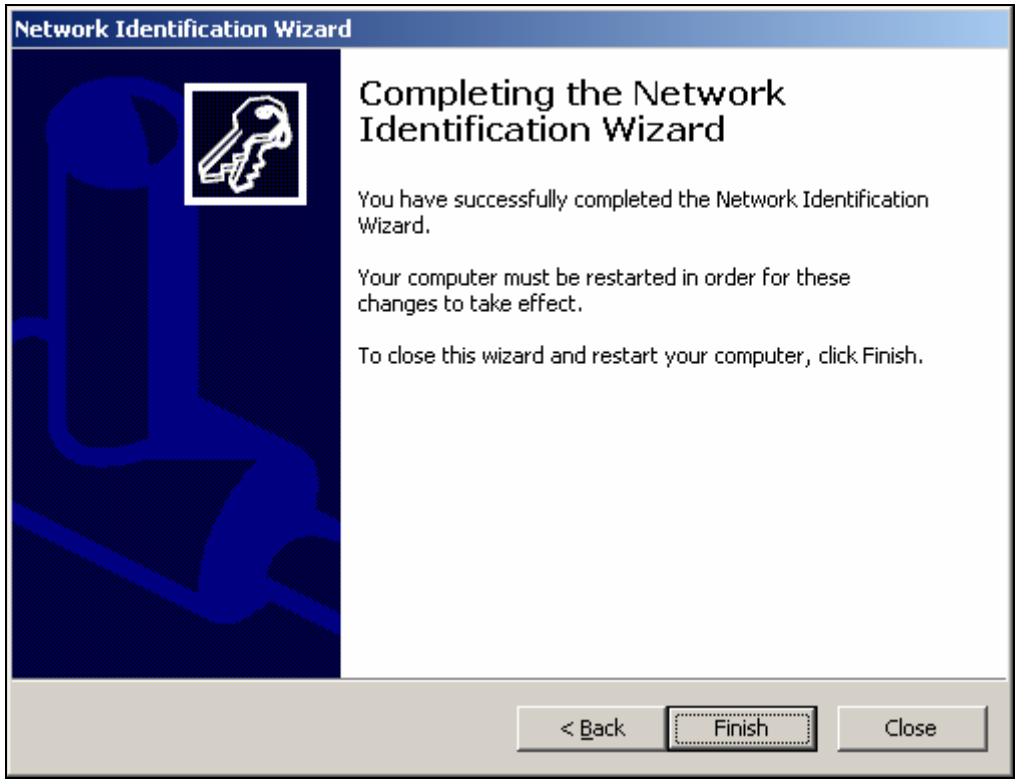

Figure 37: Network Identification Wizard Screen.

21. Double-click *Users and Passwords* within Control Panel. Deactivate the *Users Must Enter a User Name and Password …* checkbox. Click *Apply*.

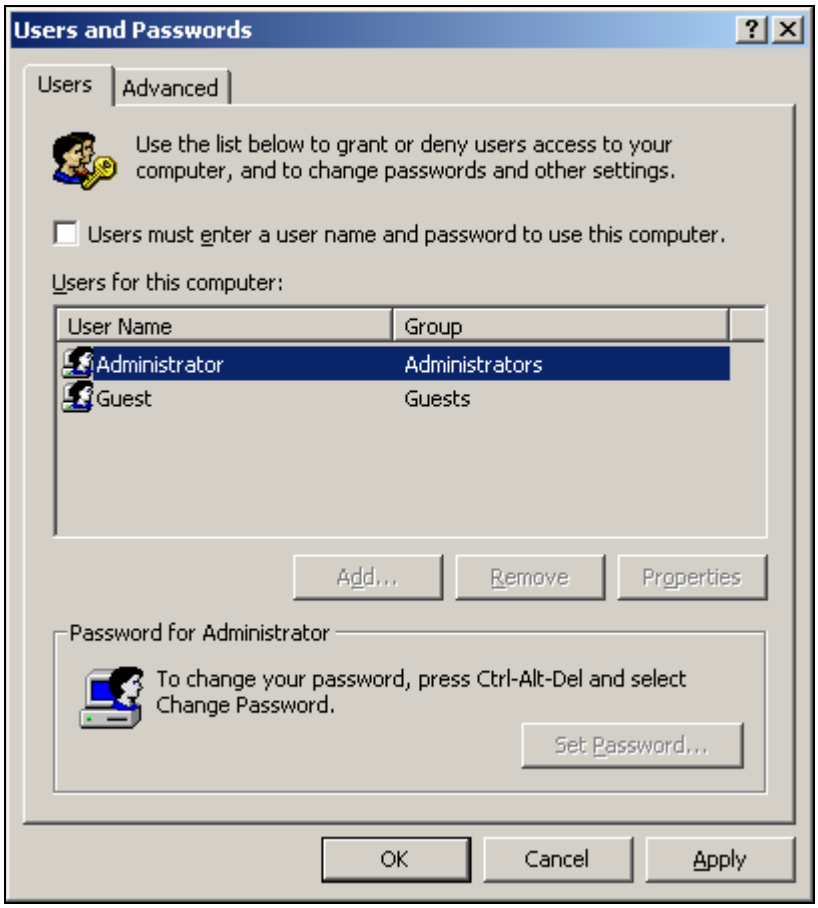

Figure 38: Users and Passwords Screen.

22. Type *Administrator* in the User Name field. Type the system's password in the Password and Confirm Password textbox. In this example, the password is [*blank*]. Click *Ok.* Click *Ok* on the Users and Passwords screen.

Figure 39: Automatic Logon Screen.

23. Repeat the Windows 2000 SP4 procedure for any other Windows 2000 SP4 system that may communicate using the *Remote MBX Driver*.